REPUBLIQUE DU CAMEROUN
Paix-Travail-Patrie

MINISTERE DES POSTES ET TELECOMMUNICATIONS

SECRETARIAT GENERAL

DIRECTION DES AFFAIRES GENERALES

REPUBLIC OF CAMEROON
Peace-Work-Fatherland

MINISTRY OF POSTS AND TELECOMMUNICATIONS

GENERAL SECRETARIAT

DEPARTMENT OF GENERAL AFFAIRS

AVIS D'APPEL A MANIFESTATION D'INTERET N° 00000008/AMI/MPT/SG/DAG/SDBM/SMA/2020 DU 13 AVR 2020 POUR LA PRESELECTION DES CABINETS D'ETUDES OU ENTREPRISES POUR LA REALISATION DES ETUDES DE FAISABILITE EN VUE DE LA MISE EN PLACE D'UN SYSTEME DE SECURISATION NUMERIQUE DES DOCUMENTS DU MINPOSTEL (SECURDOC).

1. Contexte et justification

A l'heure où le monde entre dans l'ère de l'industrie 4.0 (la révolution du numérique), tous les domaines d'activités convergent vers le « tout numérique ». Le plus grand défi est la protection et la préservation des données. Dans le plan stratégique Cameroun numérique 2020, notre pays envisage, dans son troisième axe stratégique, la transformation numérique de l'administration et des entreprises et principalement le renforcement de la confiance numérique dans son cinquième axe. Partant du constat selon lequel le pays connait de nombreuses entraves sécuritaires, des fuites de documents administratifs sur les média sociaux, il est crucial de mettre un accent sur la sécurisation dans la gestion des documents au sein de l'appareil étatique, comme le rappelait le Premier Ministre dans la circulaire N°003/CAB/PM du 28 mars 2018 relative à la gestion des documents et données confidentiels de l'Etat et des organismes du secteur public.

Prenant particulièrement le cas du MINPOSTEL, le traitement des dossiers au sein de cette structure nécessite, la prise en compte des aspects liés à la confidentialité, l'intégrité, la disponibilité, la non répudiation, l'authentification des documents et la mise en place d'un système de gestion physique et numérique des documents tel que stipulent la loi N°2000/010 du 19 Décembre 2000 régissant les archives au Cameroun et son décret d'application N°2001/958/PM du 1er novembre 2001 et le décret d'application N° 2012/1318/PM du 22 mai 2018 de la loi N° 2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun.

Dans l'optique d'impulser la dématérialisation des procédures et documents physiques administratifs et de les sécuriser, ce projet s'oriente selon deux axes du « plan stratégique Cameroun 2020 » à savoir, assurer la transformation numérique de l'administration et des entreprises (axe 3) renforcer la confiance numérique (axe 5). En outre, il s'ancre au DSCE à travers la « Gestion stratégique de l'Etat » en son point « Poursuite de la modernisation de l'administration publique ». L'installation d'un tel outil permettra de résorber un large éventail de problèmes présents au sein des administrations publiques.

Cet état des choses montre à suffisance la nécessité de la mise en place d'une plateforme sécurisée (qui passe par une étude de faisabilité) qui permettra de baliser tout le processus de traitement d'un dossier administratif, de la version papier à la version numérique, de sa création à sa conservation, conformément aux dispositions règlementaires nationales et aux normes internationales, surtout que cette idée s'arrime au développement du projet e-GOV.

2. Consistance des prestations

Les prestations objets de cette étude consistent en la réalisation des tâches suivantes :

2.1. Plan technique et technologique

- Effectuer un état des lieux relatif aux procédures de sécurisation et de gestion des documents au MINPOSTEL ;
- Effectuer un audit préalable du bâtiment du MINPOSTEL afin de repérer les locaux d'archives, le câblage existant, les cheminements possibles des futurs câbles, l'emplacement éventuel du local technique et le volume moyen de données qui transite au sein du réseau du MINPOSTEL ;
- Définir et décrire les caractéristiques (nature, topologie, système de câblage, connectique, plan d'adressage, débit) du réseau de communications électroniques à installer ;
- Évaluer la taille du réseau en termes de nombre de postes de travail, longueur totale du câblage, nombre d'équipements réseaux (routeurs, switchs, serveurs…) et le nombre d'équipements électriques (prises de courant, onduleurs, éclairage, camera…) ;
- Définir et décrire les caractéristiques et l'organisation du local technique (superficie, emplacement, type de revêtement, mobilier, structure des portes et fenêtres, température et humidité) ;
- Élaborer un plan d'aménagement du local technique qui devra mettre l'accent sur les installations électriques, les systèmes d'éclairage, d'aération, de climatisation, d'hygrométrie, d'alerte incendie, de détection de présence, de biométrie et de vidéosurveillance ;
- Définir et décrire les types de rayonnages destinés à la conservation des documents d'archives ;
- Identifier les processus métiers ainsi que les acteurs qui sont impliqués ;
- Définir la charte de développement et de validation des applications de la solution ;
- Définir les formats et les caractéristiques numériques des documents ;
- Définir et décrire les workflows du circuit de validation d'un document de sa création à son archivage ;
- Décrire l'ensemble des fonctionnalités, modules et services de la solution ;
- Décrire de façon claire le processus de collecte, de traitement, d'archivage et de destruction des documents ;
- Définir les spécificités et décrire le processus de numérisation des documents ;
- Définir les spécificités et décrire le processus de traitement des documents (classification, référencement, indexation…) ;
- Définir et décrire le processus de stockage des données et d'archivage des documents, en tenant compte des risques d'accidents et de pannes ;
- Identifier et décrire de façon précise et claire chacune des technologies, méthodes et outils qui seront utilisés pour la conception, le développement, les tests et le déploiement de la solution ;
- Élaborer un plan d'actions précis qui détaillera le chronogramme de conception, de développement, de test et de déploiement de la solution (séquencement, produits, services, méthodes de validation de produits) ;
- Décrire de façon précise le mécanisme visant à garantir l'interopérabilité de la solution ;
- Définir et décrire les mécanismes du système de Gestion Electronique des Documents (GED) qui aident à assurer la confidentialité, l'intégrité et la disponibilité des données (chiffrement, contrôle d'accès, certificats SSL, authentification et signature électronique);
- Définir et décrire un mécanisme d'authentification spécifique aux documents numérisés basé sur la signature électronique et la technologie de QR (Quick Response) Code ;
- Élaborer un plan directeur d'administration et de contrôle du réseau de communications électroniques qui devra prendre en charge la gestion des pannes, l'allocation statique et dynamique de la bande passante, les droits d'accès au réseau et la surveillance du réseau ;

- Définir et décrire les technologies et les outils permettant l'interconnexion du réseau à Internet ;
- Définir et décrire les technologies et outils garantissant la sécurisation du réseau de communications électroniques ;
- Définir et décrire les technologies et outils d'évaluation en temps réel du niveau de vulnérabilités du réseau ;
- Définir et décrire les technologies et outils de correction en temps réel des vulnérabilités du réseau ;
- Élaborer l'architecture globale de la solution ;
- inventorier et décrire l'ensemble des documents existant en dissociant les documents d'archives de ceux destinés à la bibliothèque et à la documentation, ainsi que les documents courants des documents d'archives définitives (CEDOC : Centre de la Documentation et des Archives, Courrier central, Courrier du Cabinet, DSR : Direction de la Sécurité des Réseaux et des Systèmes d'information et les Services Déconcentrés).

2.2. Formations et renforcement des capacités

- Il s'agit dans cette phase, d'élaborer un syllabus de formation en vue d'appuyer et de renforcer les capacités du personnel en charge de la solution, sur l'élaboration du support de formations détaillées au profit des différentes catégories de personnel (technique, administratif, etc) ;
- Le syllabus devra définir les approches de formation théoriques et pratiques. L'aspect théorique concernera la présentation des fonctionnalités de la solution, et la présentation du retour d'expérience sur les bonnes pratiques en matière de GED.

2.3. Gestion du changement

Analyser les risques auxquels la solution sera confrontée, faisant un focus sur la résistance au changement dans l'optique de la GED. À cet égard, il faudra en matière de gestion de changement, définir des mesures et des mécanismes de gestion desdits risques afin de les atténuer ou de les annuler.

2.4. Communication

La mise en œuvre de ce projet doit être accompagnée d'une stratégie et d'un plan stratégique de communication en vue de la sensibilisation sur l'importance de l'utilisation de la solution.

2.5. Plan de qualité de service

- Définir la méthodologie mise en place pour satisfaire le besoin exprimé par le bénéficiaire de la solution ;
- Définir la liste des valeurs mesurables permettant d'exprimer de manière factuelle le niveau du service de la solution ;
- Décrire la façon dont sera organisée les relations entre les Parties (maitre d'ouvrage, maitre d'œuvre) ;
- Présenter la liste des tâches qui incomberont à chaque Partie ainsi que les niveaux de service sur lesquels le bénéficiaire s'engagera pour la réalisation de la solution.

3. Participation

Pour faire acte de candidature, tout Cabinet d'Etude ou Entreprise, devra justifier d'une expérience avérée dans le domaine des TIC de la cybersécurité et de la protection des réseaux et des systèmes d'information et d'audit de sécurité.

4. Composition du dossier de candidature

Le dossier d'Avis à Manifestation d'Intérêt comprendra les sections suivantes :

- Section 1 : Pièces administratives ;
- Section 2 : Dossier technique.

4.1. Section 1 : pièces administratives (enveloppe A)

La section 1 comprend les pièces administratives (originales ou leurs copies certifiées conformes datant de moins de trois (03) et valables pour l'exercice en cours) suivantes :

a) lettre de motivation dûment signée du soumissionnaire ;
b) copie certifiée, par le service des impôts, de la carte de contribuable ;
c) copie du registre du commerce, certifiée au greffe du tribunal de 1ère instance ;
d) attestation de non redevance (copie certifiée, par le service des impôts)
e) attestation de non exclusion des marchés publics délivrée par l'ARMP ;
f) attestation de non faillite (original ou copie certifiée par le greffe du tribunal de 1ère instance ;
g) attestation de soumission à la CNPS délivrée par un responsable habilité.

4.2. Section 2 : dossier technique (enveloppe B)

L'enveloppe B contiendra les informations suivantes :

- la présentation du cabinet ainsi que les domaines d'action et d'intervention ;
- la liste du personnel clé avec les copies des diplômes et des CV datés et signés par chaque expert ;
- les références du Cabinet d'Etudes pour les prestations similaires réalisées au cours des cinq (05) dernières années ;
- la compréhension du mandat de mission (TDR)

5. Critères d'évaluation et de sélection des cabinets

5.1. Critères éliminatoires

N°	Désignations
01	Dossier administratif incomplet
02	Fausse déclaration, document falsifié
03	Note technique inférieure à 75 points sur 100

5.2. Critères de qualification

Les offres techniques seront présentées en fonction des principaux critères ci-après :

a) **Compréhension du mandat de la mission (contexte, objectifs, méthodologie, résultats, planning de réalisation) 20 points ;**
b) **Expérience du cabinet (au moins 05 ans dans la réalisation des prestations du domaine des TIC) 05 points ;**
c) **Expérience du personnel clé 45 points**

N°	Désignations	Notation
01	L'expérience du personnel clé. • Un (1) Chef de projet, documentaliste ou archiviste, BAC+ 5 minimum, avec au moins 10 ans d'expérience, ayant déjà conduit au moins cinq (05) projets similaires au cours des cinq dernières années. ……………………………15 pts; • Un (1) Expert sécurité informatique, Ingénieur en TIC (Informatique ou télécoms) BAC+5, avec au moins 05 ans d'expérience en sécurité des réseaux et des systèmes d'information et doté d'une certification en cryptologie …………………………………………………7.5 pts; • Un (1) Expert, Ingénieur informaticien BAC+5, expert en Sécurité des réseaux et systèmes d'information (une expérience en cryptologie)…………………7.5 pts; • Un (1) Ingénieur informaticien ou équivalent (BAC+5), avec au moins 5 ans d'expérience en sécurité informatique (couche réseau et couche applicative) et des applications en ligne et doté d'une très bonne connaissance des normes de sécurité applicative (ISO27034). ……………………………………7.5 pts; • Un (01) Ingénieur en TIC (Informatique ou télécoms), BAC+5, avec au moins 5 ans d'expérience en sécurité des réseaux et des systèmes d'information, au moins un certificat en sécurité informatique (CCNA Security, CCSP ou CISSP)..7.5 pts.	45

	<u>NB</u> : L'expérience du personnel clé est justifiée par la copie certifiée du diplôme et le CV daté et signé par l'expert).	

d) Références du candidat **30 points**

N°	Désignation	Notation
01	Les références du Cabinet d'Etudes pour les prestations similaires réalisées au cours des cinq (05) dernières années (fournir les preuves de la réalisation des missions similaires (système d'information)) : 15 points par référence.	30
	Total	**30**

Récapitulatif des critères de qualification

N°	Critères	Notation
a	Compréhension du mandat de la mission	20
b	Expérience du cabinet	05
c	Expérience du personnel clé	45
d	Références du candidat	30
	Total	**100**

6. Dépôt des dossiers

Les dossiers de candidature seront remis en cinq (05) exemplaires dont un (01) original et quatre (04) copies marquées comme tels, sous pli fermé scellé et comportant deux enveloppes distinctes à la Direction des Affaires Générales, Service des Marchés (porte 162), au Ministère des Postes et Télécommunications, au plus tard le 25 MAI 2020 à 14 heures 30 minutes, heure locale et devra porter la mention :

AVIS D'APPEL A MANIFESTATION D'INTERET
N°______________/AMI/MPT/SG/DAG/SDBM/SMA/2020 DU ______________ POUR LA PRESELECTION DES CABINETS D'ETUDES OU ENTREPRISES POUR LA REALISATION DES ETUDES DE FAISABILITE EN VUE DE LA MISE EN PLACE D'UN SYSTEME DE SECURISATION NUMERIQUE DES DOCUMENTS DU MINPOSTEL (SECURDOC).

« A n'ouvrir qu'en séance de dépouillement »

7. Renseignements complémentaires

Les renseignements complémentaires peuvent être obtenus aux heures ouvrables au Ministère des Postes et Télécommunications, Direction de la Sécurité des Réseaux et des Systèmes d'Information, porte 108, Ministère des Postes et Télécommunications, bâtiment annexe. Tél : 222 23 29 75 / 242 74 27 67.

8. Publication des résultats

L'Avis d'Appel d'Offres National Restreint (AONR) fera office de publication des résultats du présent avis d'Appel à Manifestation d'Intérêt./-

Le Ministre des Postes et Télécommunications

Le Ministre
The Minister

Mme Libom Li Likeng
née Mendomo Minette

REPUBLIQUE DU CAMEROUN
Paix-Travail-Patrie

MINISTERE DES POSTES ET TELECOMMUNICATIONS

SECRETARIAT GENERAL

DIRECTION DES AFFAIRES GENERALES

REPUBLIC OF CAMEROON
Peace-Work-Fatherland

MINISTRY OF POSTS AND TELECOMMUNICATIONS

GENERAL SECRETARIAT

DEPARTMENT OF GENERAL AFFAIRS

CALL FOR EXPRESSION OF INTEREST No. 0000008/AMI/MPT/SG/DAG/SDBM/SMA/2020 OF 03 AVR 2020 FOR THE ESTABLISHMENT OF A SHORT-LIST OF CONSULTING FIRMS OR COMPANIES TO CONDUCT FEASIBILITY STUDIES IN VIEW OF SETTING UP A DIGITAL SECURITY SYSTEM FOR MINPOSTEL DOCUMENTS (SECURDOC).

1. Background and justification

At the time when the world enters the era of Industry 4.0 (the digital revolution), all fields of activity are converging towards the principle "all-digital technologies". The greatest challenge is the protection and preservation of data. In the Strategic Plan for a digital Cameroon by 2020, our country considers, in its third strategic axis, the digital transformation of administrations and companies and mainly the enhancement of digital confidence in its fifth axis. Based on the observation that the country is experiencing many security problems, leaks of administrative documents, which are sometimes confidential, on social media, it is crucial to focus on security in the management of documents within the state apparatus, as recalled by the Prime Minister in Circular No. 003/CAB/PM of 28 March 2018 on the management of confidential documents and data of the State and public sector organisations.

Considering in particular the case of MINPOSTEL, the processing of files within this structure requires that aspects related to confidentiality, integrity, availability and non-repudiation be taken into account, the authentication of documents and the establishment of a physical and digital document management system as stipulated in Law No. 2000/010 of 19 December 2000 to govern archives in Cameroon and its implementing Decree No. 2001/958/PM of 1 November 2001 and implementing Decree No. 2012/1318/PM of 22 May 2018 of Law No. 2010/013 of 21 December 2010 to govern electronic communications in Cameroon.

In order to boost the dematerialisation of administrative procedures and physical documents and to secure them, this project is geared towards two axes of the "Strategic Plan for a Digital Cameroon by 2020" namely, to ensure the digital transformation of administrations and enterprises (axis 3) and to enhance digital confidence (axis 5). In addition, it is anchored in the GSEP through the "Strategic Management of the State" in its section "Continuing the modernisation of public administration". The installation of such a tool will make it possible to resolve a wide range of problems present within public administrations.

This situation sufficiently highlights the need for the implementation of a secure platform (which requires a feasibility study) that will make it possible to mark out the entire process of processing an administrative file, from the paper version to the digital version, from its creation to its conservation, in accordance with national regulatory provisions and international standards, especially as this idea is linked to the development of the e-GOV project.

2. Description of services

The services under this study consist in the conduct of the following tasks:

2.1. Technical and Technological Plan

- Conduct an inventory of the security and document management procedures at MINPOSTEL;
- Conduct a preliminary audit of the MINPOSTEL building in order to identify archive premises, existing cabling, possible routes for future cables, the possible location of the technical room and the average volume of data transiting within the MINPOSTEL network;
- Define and describe the characteristics (nature, topology, cabling system, connections, addressing plan, flow rate) of the electronic communications network to be installed;
- Evaluate the size of the network in terms of number of workstations, total length of cabling, number of network equipment (routers, switches, servers...) and the number of electrical equipment (sockets, inverters, lighting, camera...);
- Define and describe the specifications and organisation of the technical room (surface area, location, type of cladding, furniture, doors and windows structure, temperature and humidity) ;
- Draw up a layout plan for the technical room which should focus on electrical installations, lighting, ventilation, air conditioning, hygrometry, fire alarm, presence detection, biometrics and video surveillance systems;
- Define and describe the types of shelving for the storage of archival documents;
- Identify the business processes and the stakeholders involved;
- Define the development and validation charter for the solution's applications;
- Define the formats and digital specifications of the documents;
- Define and describe the workflows of the validation circuit of a document from its creation to its archiving;
- Describe all the functionalities, modules and services of the solution;
- Describe in a concise manner the process of collecting, processing, archiving and destroying documents;
- Define the specificities and describe the process of document digitization;
- Define the specificities and describe the document processing procedure (classification, referencing, indexing...);
- Define and describe the process of data storage and archiving of documents, taking into account the risks of accidents and breakdowns;
- Identify and describe precisely and clearly each of the technologies, methods and tools that will be used for the design, development, testing and deployment of the solution;
- Develop a precise action plan that will detail the timeline for the design, development, testing and deployment of the solution (sequencing, products, services, product validation methods);
- Describe precisely the mechanism to ensure the interoperability of the solution;
- Define and describe the mechanisms of the Electronic Document Management (EDM) system that help ensure data confidentiality, integrity and availability (encryption, access control, ssl certificates, authentication and electronic signature);
- Define and describe a specific authentication mechanism for scanned documents based on electronic signature and Quick Response (QR) Code technology;
- Develop a master plan for the administration and control of the electronic communications network that will address fault management, static and dynamic bandwidth allocation, network access rights and network monitoring;
- Define and describe the technologies and tools for interconnecting the network to Internet;
- Define and describe the technologies and tools that ensure the security of the electronic communications network;
- Define and describe the technologies and tools for real-time assessment of the level of network vulnerabilities;

- Define and describe technologies and tools for real-time correction of network vulnerabilities;
- Develop the global architecture of the solution;
- Make an inventory and describe all existing documents by separating archival documents from those intended for the library and documentation, as well as current documents from final archival documents (CEDOC : Documentation and Archives Centre, Central Mail Office, Cabinet Mail Office, DSR: Department of Security of Networks and Information Systems and External Services).

2.2. Training and capacity building

- This phase involves developing a training syllabus to support and build the capacities of personnel in charge of the solution, on the development of detailed training materials for the various categories of personnel (technical, administrative, etc.);
- The syllabus should define the theoretical and practical training approaches. The theoretical aspect has to do with the presentation of the solution features and the presentation of the feedback on GED best practices

2.3. Change Management

Analyse risks related to the solution, while laying emphasis on resistance to change from the GED perspective. In this regard, it will be necessary to define change management measures and mechanisms to manage these risks in order to mitigate or cancel them.

2.4. Communication

The implementation of this project must be accompanied by a communication strategy and strategic plan to raise awareness on the importance of using the solution.

2.5. Service Quality Plan

- Define the methodology set up to meet the need expressed by the beneficiary of the solution;
- Define the list of assessable values allowing the service level of the solution to be expressed in a factual manner;
- Describe the way in which the relations between the Parties will be organised (project owner, project manager);
- Present the list of tasks that will be assigned to each Party as well as the levels of service to which the beneficiary will commit for the realisation of the solution.

3. Participation

In order to apply, any Consulting firm or company must have proven experience in the field of ICT, and relevant experience in the fields of digital and physical archiving, network and information system security and the development of distributed and centralised information systems.

4. Application file

The application file of the Call for Expression of Interest shall include the following volumes:

- Volume 1 : Administrative documents;
- Volume 2 : Technical documents.

4.1. Volume 1: Administrative documents (envelop A)

Volume 1 shall include the following administrative documents (originals and their certified true copies of not more than three (03) months and valid for the current financial year):

a) A cover letter duly signed by the applicant;
b) True copy of taxpayer card certified by the tax service;
c) a copy of the commercial register, certified by the Registry of the Court of First Instance;
d) tax clearance certificate (copy certified, by the tax service)
e) a certificate of non exclusion from public contracts issued by the ARMP;

f) a certificate of non-bankruptcy (original or copy certified by the Registry of the Court of First Instance;

g) a certificate of affiliation to the NSSF issued by a authorised official.

4.2. Volume 2: Technical file (envelop B)

Envelope B shall contain the following information:

- the presentation of the Firm or Consulting Firm as well as areas of action and intervention;
- the list of key staff with copies of certificates and CVs dated and signed by each expert;
- The references of the firm or consulting firm for similar works executed during the past five (05) years:
- understanding of the mission (TOR).

5. Evaluation and selection criteria of firms

5.1. Eliminatory criteria

No.	Designations
01	Incomplete administrative document
02	False declaration, forged document
03	Technical score below 75 points out of 100

5.2. Selection criteria:

The technical bids shall be presented according to the main criteria below:

a) Understanding the mandate of the mission (background, objective, methodology, results, implementation schedule) **20 points**

b) Firm's experience (at least 05 years in the performance of services in the ICT sector) 05 points;

c) Experience of key personnel **45 points**

No.	Designations	Rating
01	The experience of key personnel. • One (01) Project Manager: documentalist or archivist, at least GCE A/L+ 5, with at least 10 years of experience, who must have already conducted at least five (05) similar projects during the past five (05) years……15 pts; • One (01) Expert, IT Engineer with a GCE A/L + 5, Expert in Network and Information Systems Security (experience in cryptology will be an asset); with at least 5 years of experience……………………7.5 pts; • One (01) Expert, Network and IT System, IT Engineer or equivalent (GCE A/L+5), with at least 5 years of experience in IT System and Network, he must have participated in projects related to the area of system interconnection and data automatic transfer. ……………………………7.5 pts; • IT Engineer or equivalent (GCE A/L+5), with at least 5 years' experience in IT security (network layer and application layer) and online applications and with a very good knowledge of application security standards (ISO27034). ……………………………7.5 pts;; • One (1) IT Security Expert, One (01) ICT Engineer (IT or telecom), with at least 5 years of experience in network and information systems security, at least one certificate in IT security (CCNA Security, CCSP or CISSP) ……………7.5 pts; NB : The experience of key personnel is justified by the certified copy of the certificate and a CV dated and signed by the Expert).	45

d) Candidate's references **30 points**

No.	Designation	Rating
01	References of the consulting firm for similar works executed during the past five (05) years (show proof of the execution of similar works (information system)): 15 points/reference.	30
	Total	**30**

Summary of the qualification criteria

No.	Criteria	Rating
a	Understanding the mandate of the mission	20
b	Firm's experience	05
c	Experience of key personnel	45
d	References of candidate	30
	Total	**100**

5. Submission of files

Application files shall be submitted in five (05) copies including one (01) original and four (04) copies labelled as such, which shall be submitted in a sealed envelop containing two separate envelops to the Department of General Affairs, (room 162), at the Ministry of Posts and Telecommunications, not later than..2.6..MAI...2020.. at 2:30 pm, local time and shall carry the following label:

CALL FOR EXPRESSION OF INTEREST
No. ________________/AMI/MPT/SG/DAG/SDBM/SMA/2020 OF __________ FOR THE ESTABLISHMENT OF A SHORT-LIST OF CONSULTING FIRMS OR COMPANIES TO CONDUCT FEASIBILITY STUDIES IN VIEW OF SETTING UP A DIGITAL SECURITY SYSTEM FOR MINPOSTEL DOCUMENTS (SECURDOC).

"To be opened only during the bid-opening session"

6. Additional information

The additional information can be obtained during opening hours from the Ministry of Posts and Telecommunications, Department of Networks and Information Systems Security, Room 108, Ministry of Posts and Telecommunications, Auxiliary Building. Tel.: 242 23 29 75 / 242 74 27 67.

7. Publication of results

The Restricted National Invitation to Tender shall be published as the result of this Call for Expression of Interest./-

The Minister of Posts and Telecommunications

Le Ministre
The Minister

Mme Libom Li Likeng
née Mendomo Minette